If Emulation of Another System Is Necessary, Ensure that It Is as Correct and Complete as Possible

William L. Fithen, Software Engineering Institute [vita[3]]

2005-10-03

Incorrect or incomplete emulation can introduce vulnerability.

Description

In general, an emulation fidelity vulnerability exists when

- a system must emulate another system or device,
- that emulation is incorrect or incomplete, and
- the system uses the emulated state information to make security decisions.

The defect might be some or all of the following:

- Emulation that is too abstract. Many network-based intrusion detection systems passively watch traffic of other systems, trying to guess the state of end nodes in communications with one another based on communication fragments. Packet-based firewalls in certain configurations exhibit this same shortcoming. For both of these examples, complete emulation is not generally possible because many end-node policies that influence their state are not observable in the traffic.
- The emulator is simply wrong (i.e., logic error) and does not emulate the original correctly.
- The eumlation is correct, but it does not perform in realtime. That is, it cannot keep up with what it's emulating, resulting in a denial of service.

References

[Hoglund 04]	Hoglund, Greg & McGraw, Gary. *Exploiting Software: How to Break Code.* Boston, MA: Addison-Wesley, 2004.
[VU#548515]	Finlay, Ian. *Vulnerability Note VU#548515: Multiple intrusion detection systems may be circumvented via %u encoding*. http://www.kb.cert.org/vuls/id/548515 (2003).

SEI Copyright

[3] daisy:320 (Fithen, William L.)

Felder

Name	Wert
Copyright Holder	SEI

Felder

Name	Wert
is-content-area-overview	false
Content Areas	Knowledge/Guidelines
SDLC Relevance	Implementation
Workflow State	Publishable

[1] http://www.sei.cmu.edu/about/legal-permissions.html